EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://correoweb.mapa.es	Checks	9 pruebas
Dominio	correoweb.mapa.es	Hallazgos	39 totales
Fecha	1 de abril de 2026 a las 08:54	Problemas	9 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web muestra una puntuación de 75/100, lo que equivale a una calificación de nota B. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 2 presentaron fallos críticos relacionados con la configuración de seguridad y la infraestructura de archivos. A pesar de contar con una implementación de cifrado SSL robusta, la ausencia de cabeceras de protección activa y la exposición de información técnica comprometen la postura defensiva del servidor. En su estado actual, el sitio se considera vulnerable a ataques de inyección y reconocimiento debido a configuraciones incompletas.

Resumen de Riesgos

0	2	5	2	30
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 343 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 343 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  343 dias restantes (expira: 2027-03-10T08:29:53.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-10T08:29:53.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  No detectado
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- INFO **Tecnologias detectadas**
  ASP.NET

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 puerto(s) abierto(s), todos esperados

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
  Cerrado — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
  Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
  Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
  Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
  Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
  Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
  Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
  Cerrado — Cache Redis sin autenticacion por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
  Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: Falta esta cabecera, lo que permite la ejecución de ataques de inyección de scripts (XSS) y contenido malicioso.
[HIGH] Strict-Transport-Security: No se fuerza el uso de HTTPS, facilitando ataques de interceptación de datos y degradación de protocolo.
[MEDIUM] X-Content-Type-Options: La ausencia de esta directiva permite el sniffing de tipos MIME, aumentando el riesgo de ejecución de archivos peligrosos.
[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada en las peticiones, lo que podría filtrar rutas internas sensibles.
[MEDIUM] Permissions-Policy: No existen restricciones sobre el acceso del navegador a funciones de hardware como cámara, micrófono o geolocalización.
[MEDIUM] Archivo /readme.html: Este archivo es accesible públicamente y puede ser utilizado para identificar versiones específicas del software instalado.
[MEDIUM] Archivo /README.txt: La disponibilidad pública de este archivo técnico facilita el reconocimiento del sistema por parte de agentes externos.
[LOW] Server header expuesto: El servidor revela el uso de Microsoft-IIS/10.0, permitiendo a un atacante buscar vulnerabilidades específicas para esa versión.
[LOW] X-Powered-By expuesto: La cabecera indica el uso del framework ASP.NET, proporcionando detalles innecesarios sobre la tecnología del servidor.